FIRSTLEGAL
eDISCOVERY

eDiscovery Data Security Best Practices

CONTENTS

PERSONALIZED SOLUTIONS. EFFORTLESS EXPERIENCE. FILE THRU TRIAL™.

Introduction

When any business — especially and including law firms — shares data with an outside vendor, there needs to be assurances that there are trustworthy and safe security measures in place.

eDiscovery vendors must carefully handle your valuable data, which can include anything from confidential client information to payment systems and trade secrets.

The First Legal eDiscovery team includes security experts who understand the best practices and approaches to ensure data integrity and defend against cybercrime. We also maintain specific security policies to protect the information we handle, holding ourselves to the highest industry standards.

Our eDiscovery division interacts with sensitive data through early case assessment, document review, and beyond. We support law firms of all sizes with our expertise in keeping information compliant with legal and regulatory requirements.

If you are evaluating an eDiscovery vendor and are concerned about their security practices, read on for our insights on what to look for and which questions to ask.

Why Data Security Matters

Protecting legal clients' sensitive and personal information is critical to maintaining their trust. This is why a law firm's value and reputation are connected to effective data security.

Because the legal industry is often targeted for cyberattacks, with over a quarter of law firms reporting an attempted or successful security breach,[1] ensuring data security is a challenge.

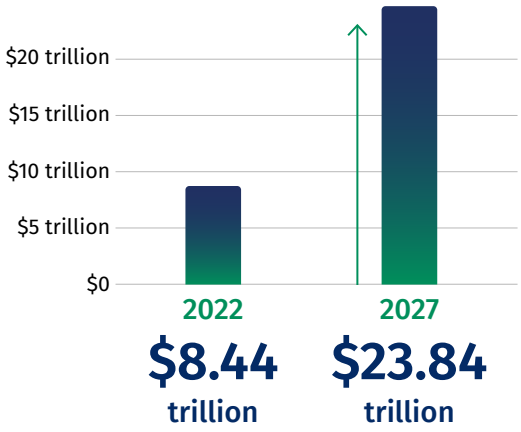
The long-term impacts of a cybercrime can be difficult to predict but they might include:

- Litigation
- Fines
- Investigation expenses
- Lost productivity
- Additional labor
- Loss of current and/or future business
- Reputational damage

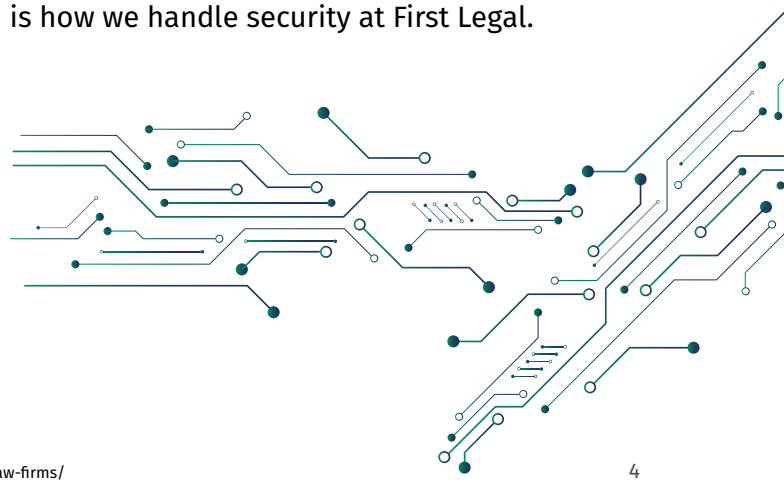
It can feel daunting trying to steer through the risks and dangers, but fortunately, there are many solutions available to help. However, deploying them is not always straightforward. While it may be tempting to use a patchwork solution of software and tools, this is not sufficient. A fully-integrated security protocol is necessary.

The Cost of Cybercime

According to the World Economic Forum, the global cost of cybercrime is predicted to jump from $8.44 trillion in 2022 to $23.84 trillion by 2027.[2]



Ideally, security is woven into every part of an organization. This way, data protection is not merely reactive, but focused on defensibility and preventing attacks before they occur. That is how we handle security at First Legal.



[1] https://www.americanbar.org/groups/law_practice/resources/tech-report/2022/cybersecurity-law-firms/
[2] https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/

Data Privacy and Protections Regulations

Depending on the type of data an organization manages and in what state it is located, there are explicit state and federal regulatory standards to adhere to. The consequences for violating these regulations vary depending on the degree of damage. For most organizations, federal and local data management laws serve as a roadmap for the correct handling of information.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA regulates the handling of sensitive health information. This standard is crucial because leaking sensitive health information can lead to identity theft, fraud, damaged business relationships, and legal penalties. Specifically, HIPAA protects individually identifiable health information and does not restrict de-identified health information.

Compliance with HIPAA "[...] requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[3] At a practical level, this means implementing policies to prevent, detect, and correct security

[3] https://www.hhs.gov/hipaa/for-professionals/security/index.html

violations. It also means conducting risk assessments regularly and training employees on the relevant security procedures.

According to the Department of Health and Human Services, organizations should "implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights."[4] Creating security policies requires the input of different departments such as IT, records, sales, and more. Consider all stages of the data's lifecycle with strategies and policies around digital storage systems, security infrastructures, backup and protection, archiving, long-term retention, and recovery.

The California Consumer Privacy Act (CCPA)

The CCPA enhances privacy rights by giving California residents control over their personal data. To be CCPA compliant, businesses must inform consumers about data collection, provide access and deletion options, offer opt-out choices for data sale, implement data security measures, and ensure non-discrimination for exercising CCPA rights.

The personal information covered by CCPA includes:

- Name, address, email address
- Social Security number
- Biometric information
- Job data
- Educational information
- Browsing history

Remaining compliant with CCPA will mean implementing a data privacy policy and updating it annually. This is because the law is likely to change over time. For example, since its implementation in 2023, consumers now have the right to correct inaccurate information about themselves.[5] It is important for this privacy policy to explain why information is collected and how to deny access to stored data.

Beyond HIPAA AND CCPA

Bloomberg Law wrote in early 2024 that there are 18 states with data protection laws in place and "such laws generally apply across industries, with exceptions for certain data categories and entity types, and grant rights to individuals pertaining to the collection, use, and disclosure of their personal data by businesses."[6] Data protection laws are constantly and quickly changing, with more states expected to enact their own, so it is important to review local regulations to ensure the correct security measures are in place to remain compliant.

[4] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf?language
[5] https://privacy.ca.gov/california-privacy-rights/rights-under-the-california-consumer-privacy-act/
[6] https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/

Questions to Ask an eDiscovery Expert About Security

While outsourcing to an eDiscovery expert can save time and money while adding convenience, it is important to have a clear conversation with eDiscovery providers about security before sharing any important data.

Establishing a systemized workflow can be more efficient than starting over with each vendor every time. Document and update this workflow with key questions relevant to your industry, the services being provided, and the risk associated with the data being shared.

Questions to ask an eDiscovery vendor before getting starting include:

1. What privacy policies and data security measures have they established? The eDiscovery expert should offer a robust explanation. Policies should cover risk management, information governance, their Security Incident Response Team (SIRT) and response plan, facility security, data handling policies, and more.

2. What kinds of data are they accustomed to accessing and processing? An eDiscovery vendor should be capable of handling and managing a wide variety of data types such as email, voicemail, PDFs, websites, social media data, photos, videos, and hard copies

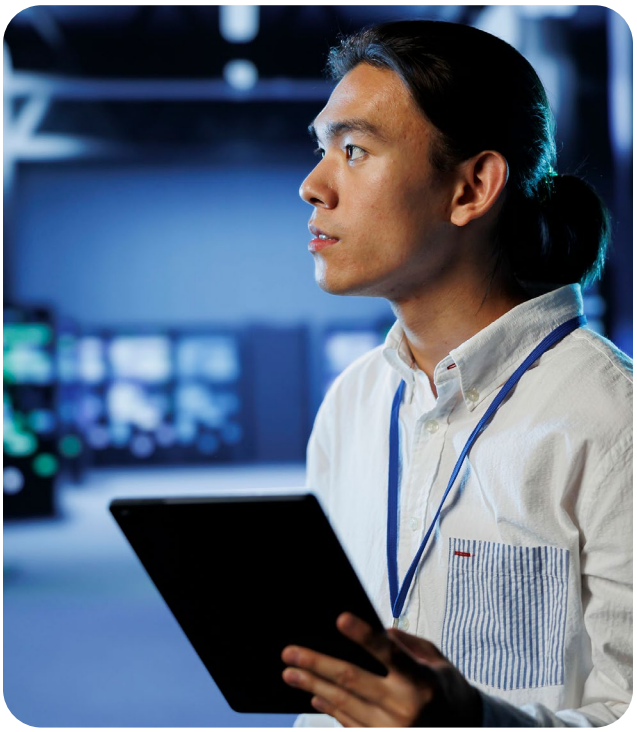
of documents. You may also wish for them to standardize different types of data.[7]

3. What kinds of offensive, defensive, and preventative strategies do they have? Look for a vendor that takes a well-rounded approach to data protection with safeguards concerning the administrative, technical, and physical sides of security.

4. Do they offer cybersecurity education and training for their employees? Cybersecurity education and training for employees is a critical component to safeguarding sensitive data from breaches and ensuring compliance with legal requirements. Some examples of employee training and education are phishing awareness, password management, data handling procedures, incident response, and more.

5. What are their cybersecurity or compliance certifications? In addition to HIPAA and CCPA mentioned previously, other certifications include the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the PCI Security Standards Council Payment Card Industry Data Security Standard (PCI DSS). Companies can also adhere to other industry standards, such as the International Organization for Standardization (ISO) 27001 series.

6. Do they conduct regular audits? To ensure ongoing compliance with data handling policies, eDiscovery vendors should perform regular audits of access permissions, encryption key management, and the effectiveness of data protection measures. Annual external audits to maintain compliance with HIPAA for the relevant data should also be conducted.



7. What is their cyber incident response plan? An incident response plan for data security is important to quickly mitigate the impact of data breaches, protect sensitive client information, and ensure compliance with legal and regulatory requirements. For an example of what an incident response plan can be, please see section No. 5 below.

8. What are their policies around secure data transfers? It is important for data to be encrypted at both ends of a transfer to keep it as safe as possible.

9. Do they have multiple points of redundancy and backups? Having a clear data retention policy is an important element of security because it minimizes the amount of data at risk by ensuring that unnecessary or outdated information is securely deleted.

[7] https://www.firstlegal.com/ediscovery-services/data-processing-hosting/

First Legal's Approach to Data Security

First Legal prioritizes in-depth defensibility, using a robust and holistic approach to data security that combines a variety of tactics, such as audits and employee education, to keep our client's information safe.

Our mature Application Security Program aligns with the Building Security in Maturity Model (BSIMM) framework and promotes security within our internal and third-party teams. We also conduct static and dynamic scans to identify any security vulnerabilities that could make our applications susceptible to an attack. We undergo regular internal and external penetration testing, which simulates what would happen in a security attack to test our network's resiliency. These tests make it more difficult for hackers to access our network and keeps our data safer.

We understand the importance of combining physical, administrative, and technical safeguards for information. Our system includes security controls at key locations to reduce the likelihood of a breach or leak of sensitive data. These controls are supplemented by setting and enforcing our specific security policies, which are explained in the next chapter.

When it comes to administrative security, First Legal ensures that only authorized personnel can access our data locations based on their role or function. This includes visitor control and those accessing our software programs for testing and revision.

To promote physical security, all on-site servers and infrastructure are monitored frequently with end-point protection. We do not retain data longer than is necessary, understanding that properly-disposed information cannot be compromised in the event of a security breach. Upon completion of a project, we obtain permission from our clients and then delete the relevant project data.

Remaining vigilant is an important aspect of our security approach, and to that end we undergo regular audits of access permissions, encryption key management, and the effectiveness of our data protection measures. We also conduct annual external audits to maintain compliance with HIPAA for the relevant data we manage. First Legal also offers monthly cybersecurity training and requires annual security training for all employees. In addition, employees who fail our phishing simulations are required to take remedial security training.

First Legal's Data Security Policies

First Legal maintains formal and documented security policies that support the ways we protect the data we manage. Our polices are designed to cover cyber security risk management, cyber security organization and governance, acceptable use, third-party vendor engagement and infosec compliance, data protection, facility security, asset management, and security risk assessment.

When creating our security policies, we looked to standard industry frameworks such as the International Organization for Standardization (ISO) 27001 to establish a structured information governance policy, standards, and security controls.[8]

> We are always re-evaluating our policies to account for changes to business practices and technological advancements.

At First Legal, we understand the need for continuous improvement and, to that end, we are working toward NIST's Cybersecurity Framework and PCI-DSS certifications.

We have comprehensive data handling policies and procedures that require when information needs to be encrypted (both in transit and at rest), safe ways to backup data, and storage protocols to ensure the highest standards of protection and compliance with legal and regulatory requirements. Data hosted in our eDiscovery division is maintained for the project's duration. Once the project is complete and confirmation from the client is received, the data is deleted. Non-hosted eDiscovery data is retained for 90 days after the invoice date and then safely erased.

We also have a risk management plan to prevent, detect, contain, and correct security violations. This is reviewed quarterly for status updates and to execute any outstanding action items. In addition, First Legal conducts a regular Security Risk Analysis (SRA). The SRA pinpoints vulnerabilities to potential unauthorized access to electronic personal health information so they can be quickly corrected.

An important part of our security procedures are our Security Incident Response Team (SIRT) and HIPAA/Information Security Officer (HSO). Our SIRT includes key personnel who are responsible for identifying and reviewing security concerns to enhance our data protection. They maintain a log of security and confidentiality matters and report on any incidents that do occur so that remedial action can be taken at once.

Like most businesses, we work with third-party vendors and understand the importance of maintaining security protocols when we do. All new third-party vendors must complete a Vendor Security Questionnaire and sign a Vendor Security Agreement before First Legal conducts business with them.

[8] https://www.iso.org/standard/27001

First Legal's Data Security Reports

New vendors should be able to offer proof that their security controls are functioning as stated. First Legal's network undergoes a series of annual tests from third-party auditors, and we have available some of the findings from our 2023's controls report. This test was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants.

System and Network Security Audit

This audit tested our network security through the physical controls in our computer rooms, data centers, and other sensitive areas. Over a dozen of our data centers from across the country were examined and found to be effective throughout the test period, which provides reasonable assurance that our system

requirements were achieved based on criteria relevant to confidentiality, integrity, and availability. These facilities were also found to be adequately equipped with environmental safeguards that protect assets and monitor for fire, water, and intrusion-related incidents. Where there was a vulnerability found, the report shows that it was remediated in a timely manner.

First Legal's security programs and business operations maintain adherence to HIPAA and PCI compliance, as well as industry expectations and other regulatory commitments.

Data Transmission Tests

All sensitive or protected data transmitted throughout our network is exchanged over secure encrypted protocols. Firewall configurations are used to ensure additional security of sensitive data during transmission. The tests verified that First Legal uses Transport Layer Security (TLS) on all public-facing URLs to ensure data protection during public transmission.

Meeting Policy Standards

The auditor verified that First Legal's documented policies are reviewed, approved, and updated annually as needed. They noted that our IT policies are based on best practice security standards, including the National Institute for Standards and Technology and ISO 27000. In addition, they confirmed that, as outlined in our data retention policy, we assign retention periods to all sensitive information.

The report also verified that First Legal has a formal incident response plan for identifying, reporting, containing, and eradicating incidents and breaches, along with the appropriate employee security training.

They also confirmed that we have an established IT business continuity policy to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

Conclusion

Ensuring robust data security when working with eDiscovery vendors is essential for law firms to protect client confidentiality and case integrity while maintaining legal compliance and safeguarding their reputation.

Rather than simply complying with the law, First Legal's eDiscovery team goes above and beyond to ensure that our clients' medical records, trade secrets, financial data, and case details are safe — just as if they were our own. We are in full compliance with PII (Personally Identifiable Information) federal and state requirements and HIPAA standards.

We never take your trust for granted and continuously re-assess our security posture to identify areas needing additional investment.

Contact us today to learn how our eDiscovery division can protect the security of your data.

Providing Services Nationally
800.772.5142
discovery@firstlegal.com
www.firstlegaldiscovery.com

FIRSTLEGAL eDISCOVERY